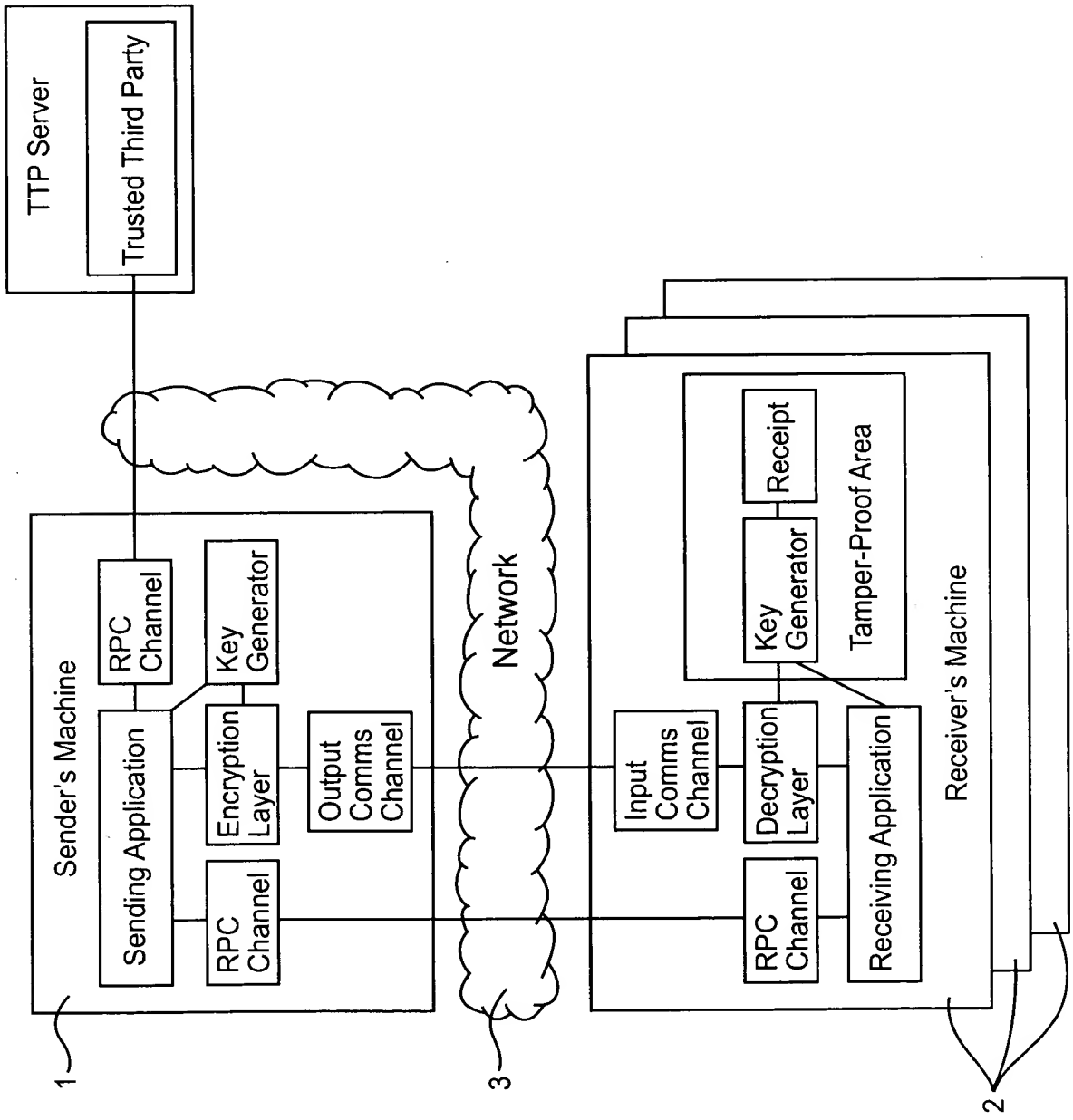
Figure 1


TTP Server
Trusted Third Party
Sender's Machine
RPC Channel
Key Generator
Sending Application
Encryption Layer
Output Comms Channel
RPC Channel
Network
Input Comms Channel
Receipt
Key Generator
Tamper-Proof Area
Decryption Layer
RPC Channel
Receiving Application
Receiver's Machine
1
3
2

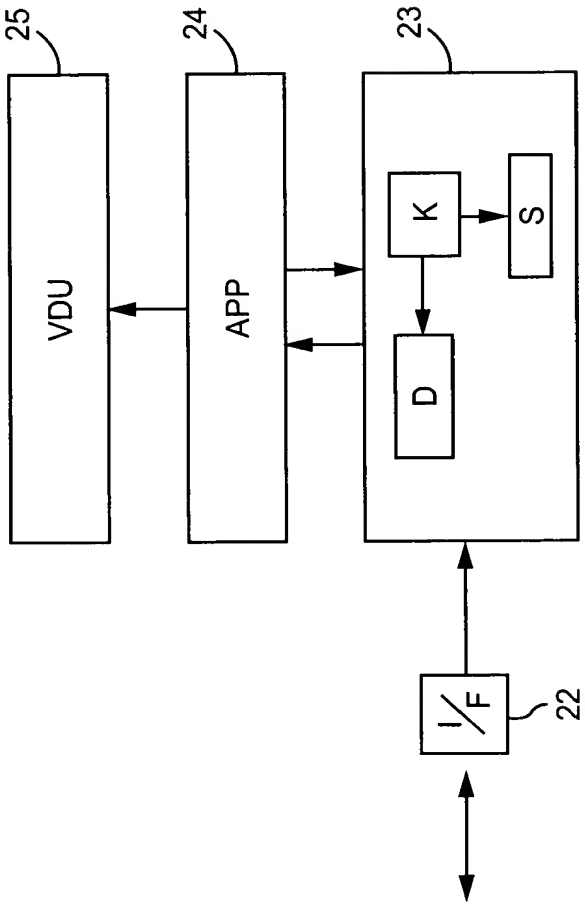


Figure 2

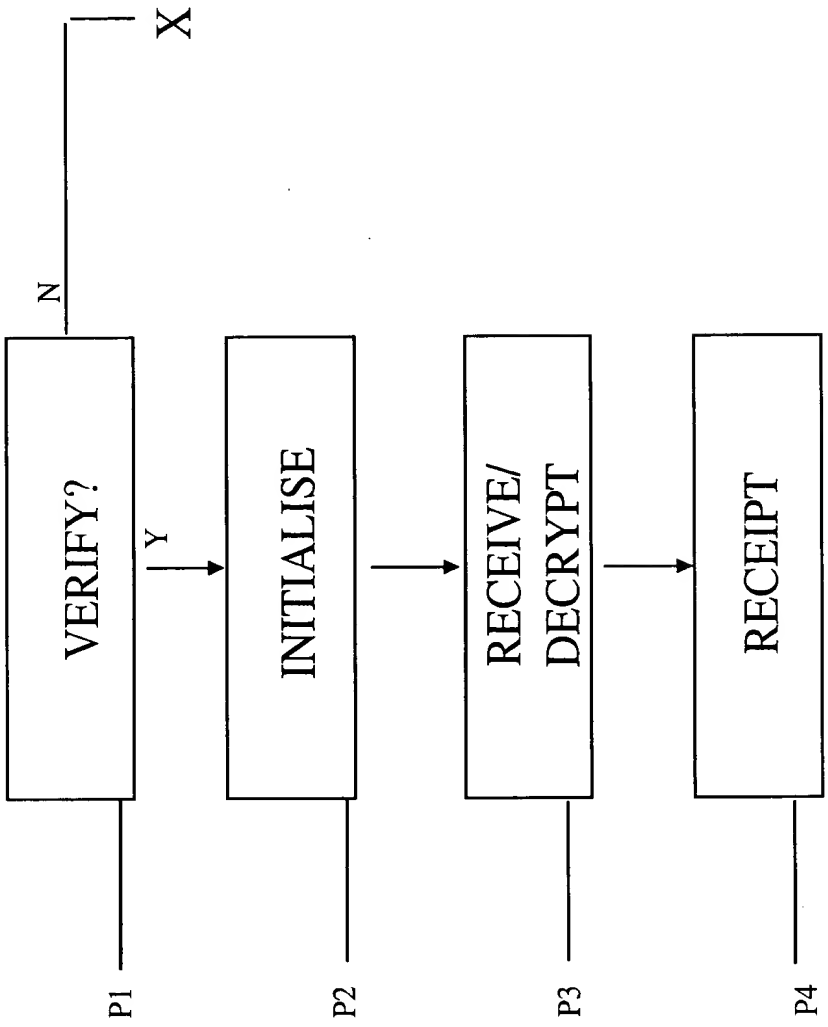


Figure 3

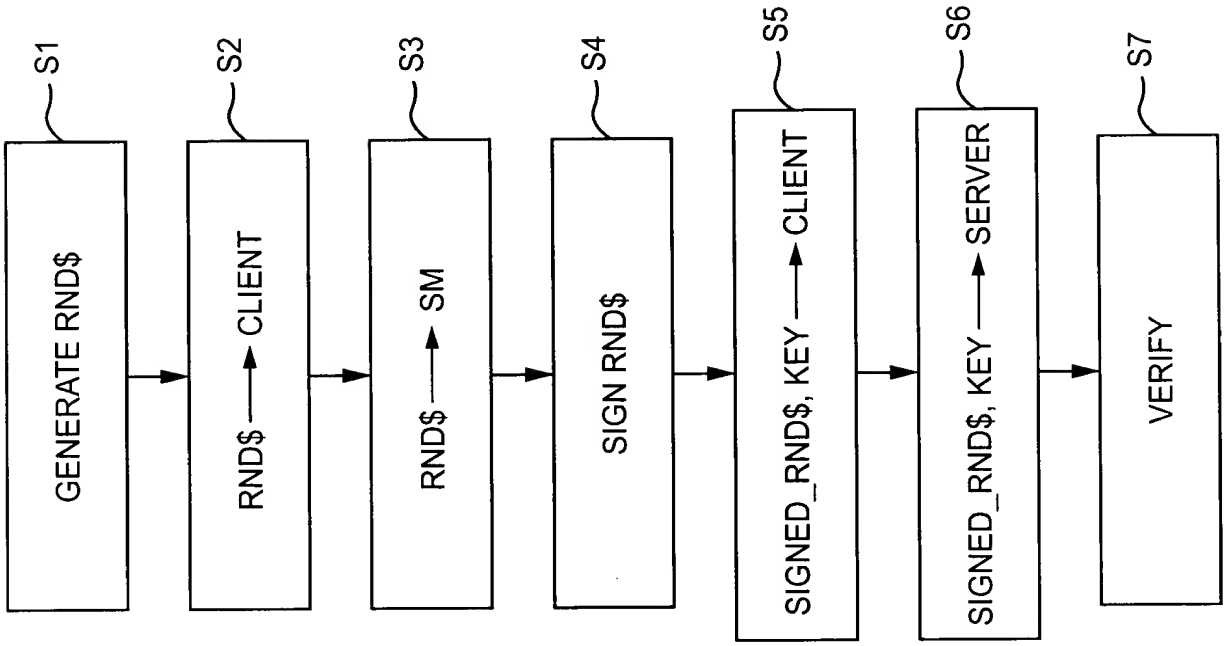

S1
GENERATE RND$
S2
RND$ → CLIENT
S3
RND$ → SM
S4
SIGN RND$
S5
SIGNED_RND$, KEY → CLIENT
S6
SIGNED_RND$, KEY → SERVER
S7
VERIFY

Figure 4

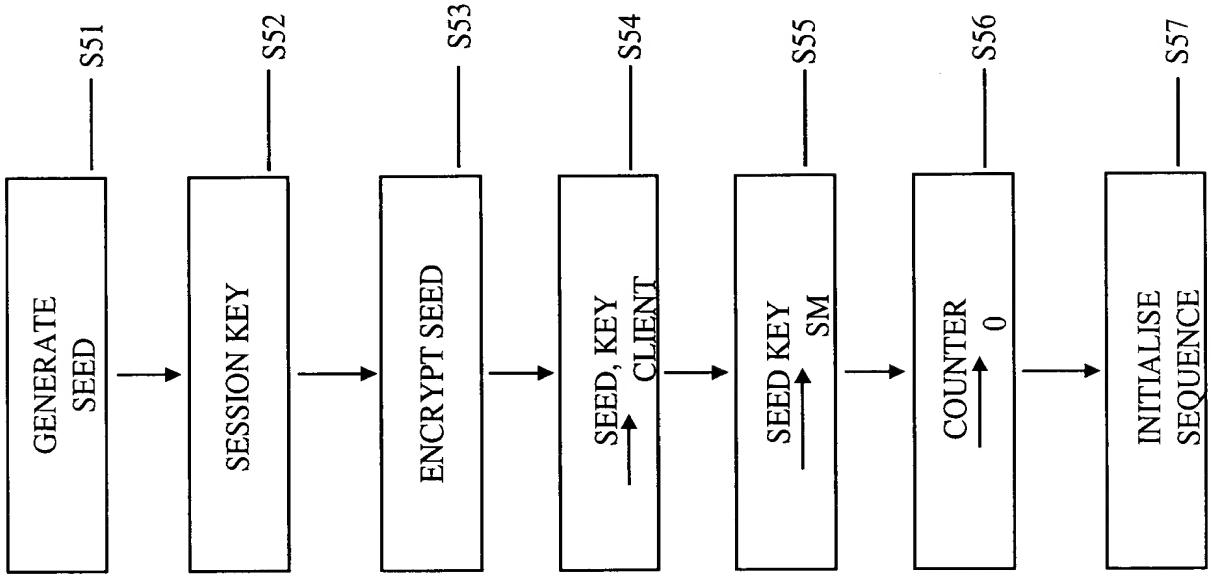

S51
GENERATE SEED
S52
SESSION KEY
S53
ENCRYPT SEED
S54
SEED, KEY CLIENT
S55
SEED KEY SM
S56
COUNTER 0
S57
INITIALISE SEQUENCE

Figure 5

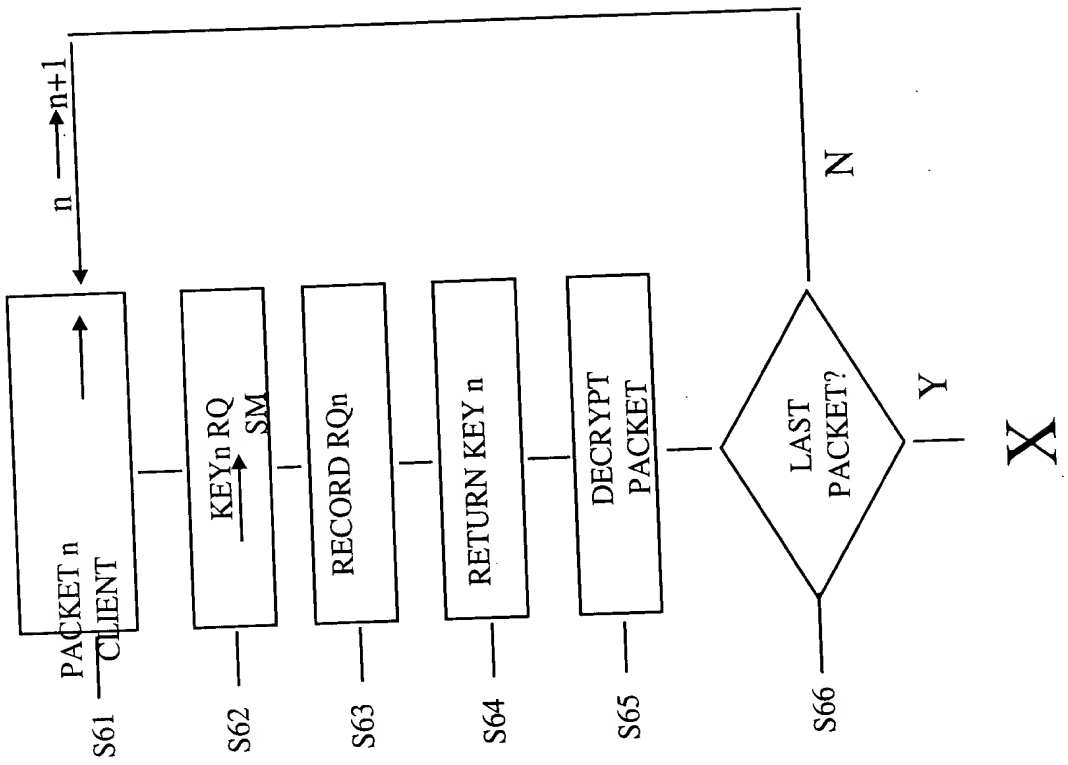

n
n+1
PACKET n
CLIENT
KEYn RQ
SM
RECORD RQn
RETURN KEY n
DECRYPT
PACKET
LAST
PACKET?
N
Y
X
S61
S62
S63
S64
S65
S66

Figure 6

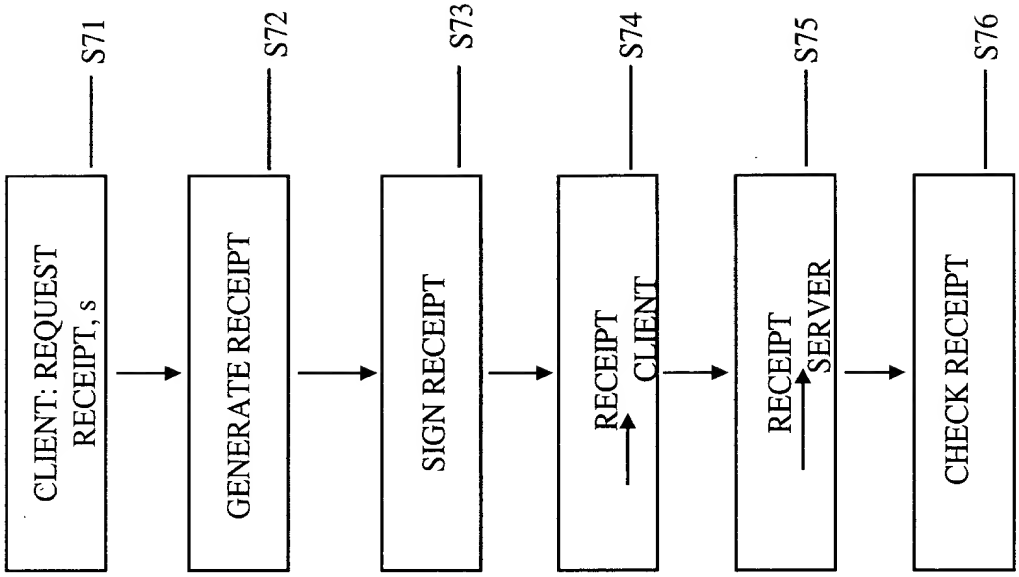

S71
CLIENT: REQUEST RECEIPT, s
S72
GENERATE RECEIPT
S73
SIGN RECEIPT
S74
RECEIPT CLIENT
S75
RECEIPT SERVER
S76
CHECK RECEIPT

Figure 7

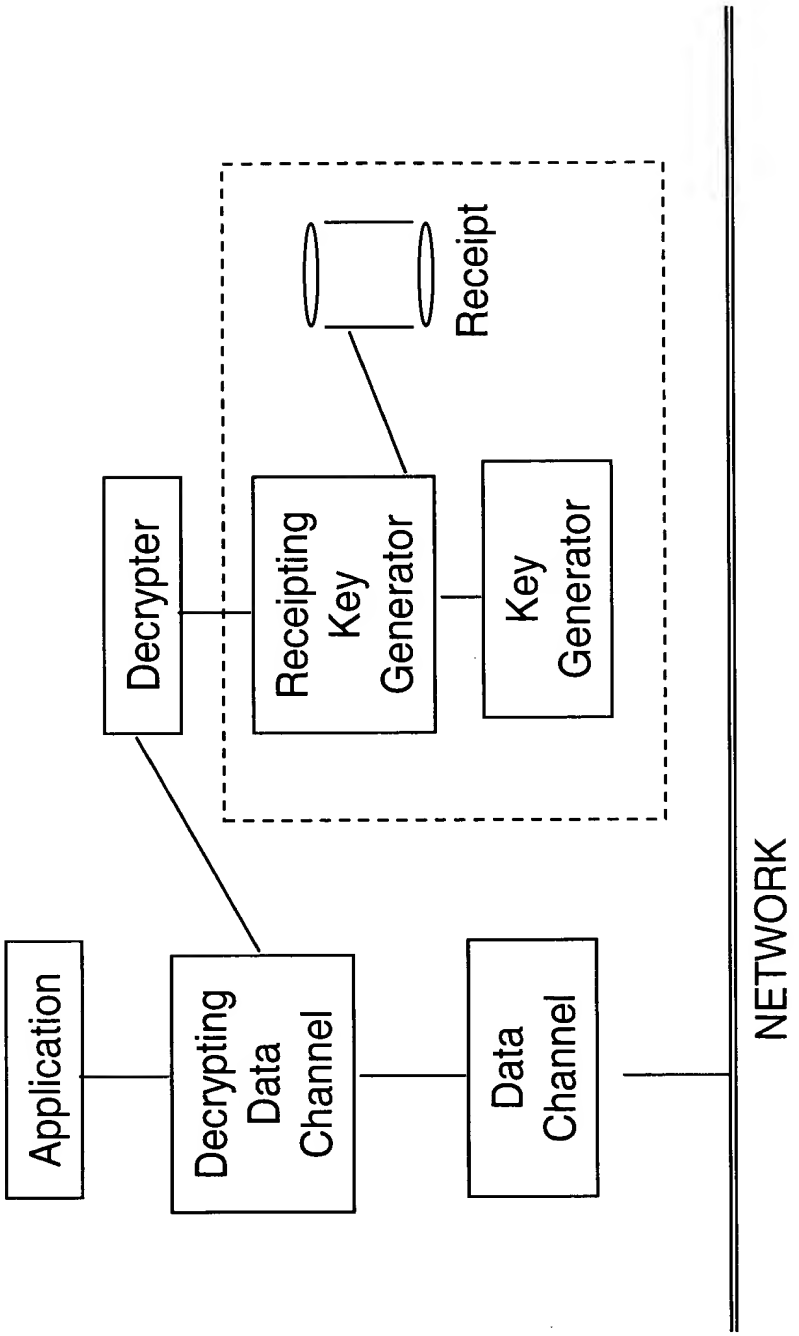

Application
Decrypting Data Channel
Data Channel
NETWORK
Decrypter
Receipting Key Generator
Key Generator
Receipt

Figure 8

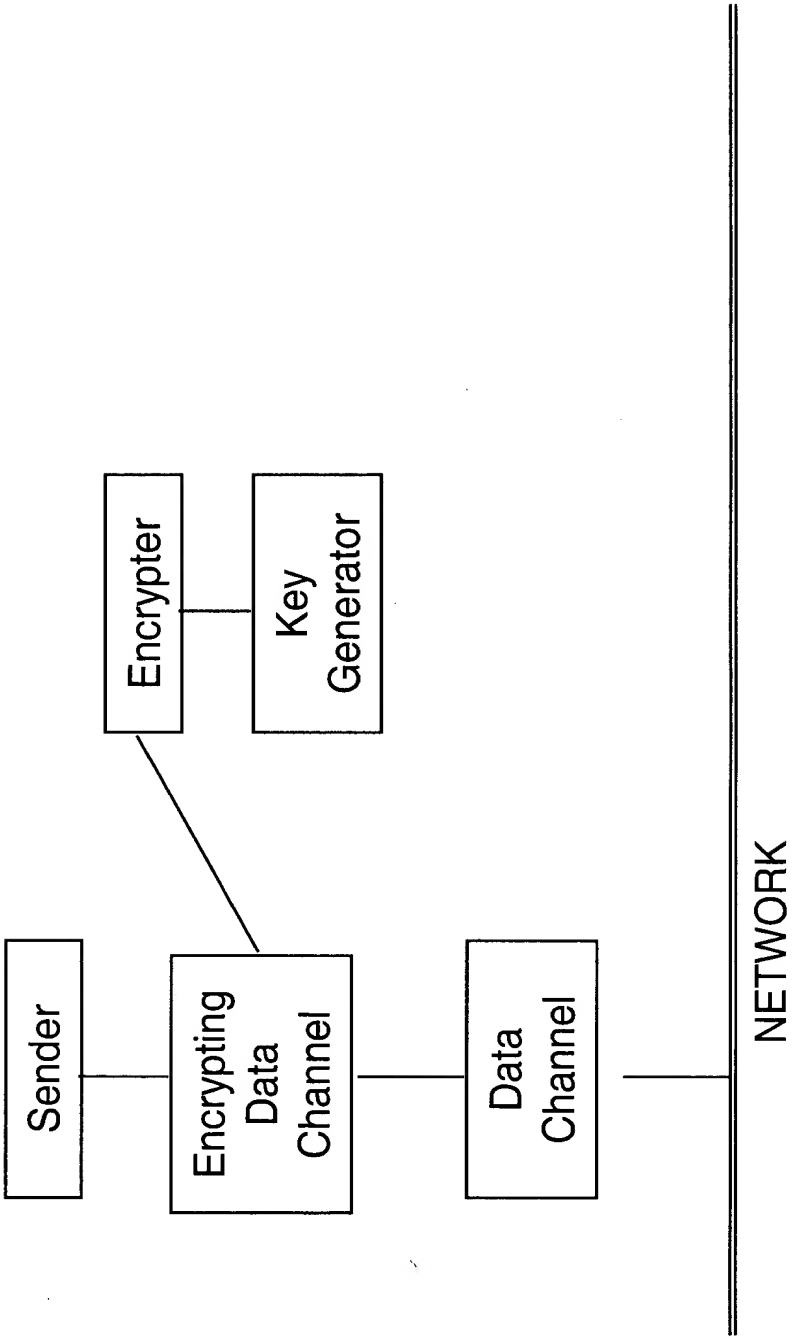

Encrypter
Key Generator
Sender
Encrypting Data Channel
Data Channel
NETWORK

Figure 9

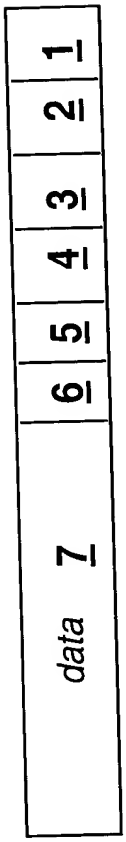


Figure 10A

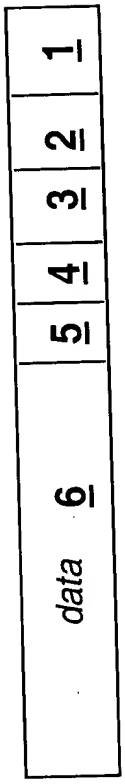


Figure 10B

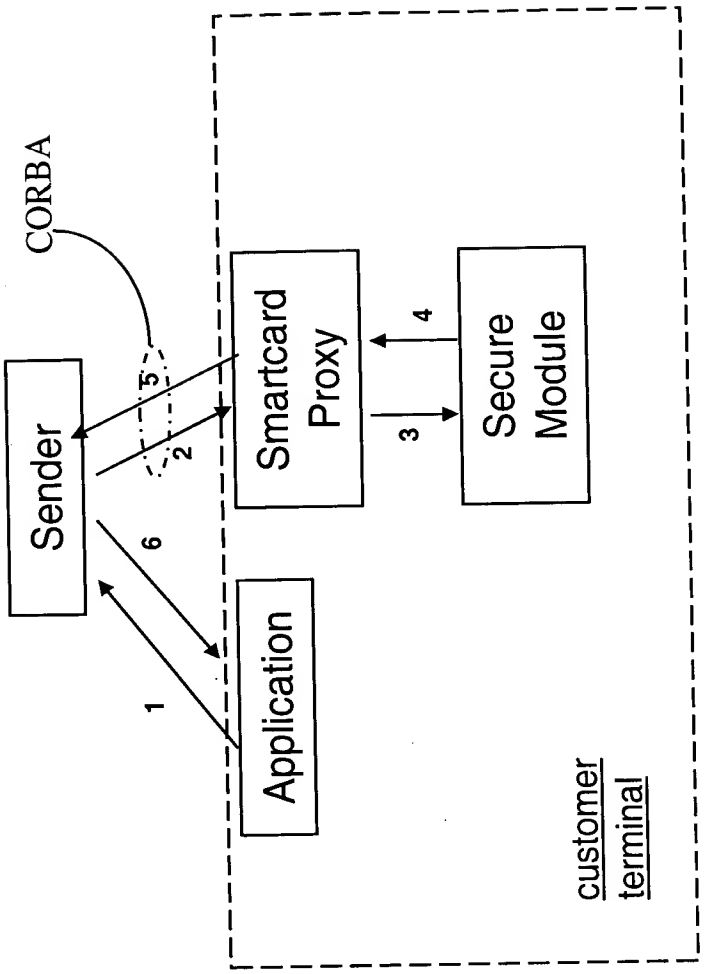
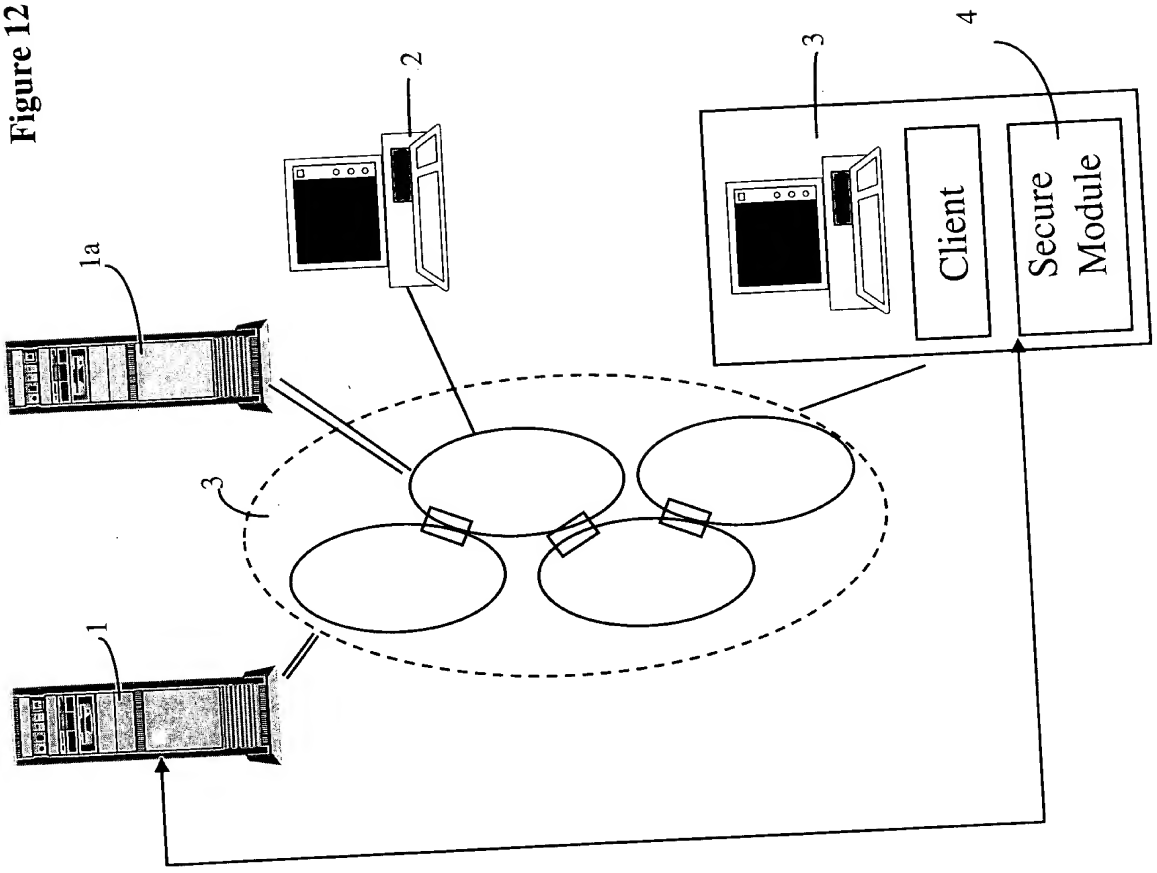

CORBA
Sender
Smartcard Proxy
Secure Module
Application
customer terminal
1
2
3
4
5
6

Figure 11

Figure 12



BEST AVAILABLE COPY